



# UNITED STATES PATENT AND TRADEMARK OFFICE

ml  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/707,100	11/20/2003	Troy Rockwood	03-0049	1099
64722	7590	04/04/2007		
OSTRAGER CHONG FLAHERTY & BROITMAN, P.C.			EXAMINER	
250 PARK AVENUE			DOAN, TRANG T	
SUITE 825				
NEW YORK, NY 10177-0899			ART UNIT	PAPER NUMBER
			2131	
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		04/04/2007	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/707,100	ROCKWOOD ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Trang Doan	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### **Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)  Responsive to communication(s) filed on 05 October 2006.

2a)  This action is **FINAL**.                            2b)  This action is non-final.

3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## **Disposition of Claims**

4)  Claim(s) 1-38 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5)  Claim(s) \_\_\_\_\_ is/are allowed.

6)  Claim(s) 1-38 is/are rejected.

7)  Claim(s) \_\_\_\_\_ is/are objected to.

8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

9)  The specification is objected to by the Examiner.

10)  The drawing(s) filed on 20 November 2003 is/are: a)  accepted or b)  objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All    b)  Some \* c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)  Notice of References Cited (PTO-892)  
2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date .  
4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_ .  
5)  Notice of Informal Patent Application  
6)  Other: \_\_\_\_ .

## DETAILED ACTION

1. Claims 1-38 are pending in this application.

### ***Claim Objections***

2. Regarding claim 1, on page 2, the Examiner interprets the limitation “a kerberos service model. wherein said plurality of nodes” as “a Kerberos service model; wherein said plurality of nodes”. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-3, 7-8, 11-14, 18, 22-24, 29-30, 32-34, 36 and 38 rejected under 35 U.S.C. 103(a) as being unpatentable over Juitt et al. (US 7042988) (hereinafter Juitt) as in view of Doshi et al. (US 6130875) (hereinafter Doshi).

5. Regarding claim 1, Juitt discloses a distributed authentication infrastructure including a plurality of nodes in communication with each other, each of said plurality of nodes having an identification and intended to perform a series of functions, one of said series of functions for verifying said identification of said plurality of nodes (Juitt: see figure 1A items 102 a-c); and a centralized authentication infrastructure integrated into said distributed authentication infrastructure and including a central server, said central

server being coupled to said plurality of nodes and being utilized for verifying said identification of said plurality of nodes (Juitt: see figure 1A item 117); wherein said distributed authentication infrastructure is initially implemented and said centralized authentication infrastructure is later integrated into said distributed authenticated infrastructure; wherein said distributed authentication infrastructure is selected from the group consisting of a threshold cryptography service model and a web-of-trust service model; wherein said centralized authentication system is selected from the group consisting of a public key infrastructure and a Kerberos service model; wherein said plurality of nodes include at least one of a personal digital assistant, a digital pager, a digital fax machine, a vide teleconferencing device, a wireless telephone, a portable computer, a desktop computer, and a communication device (Juitt: see figure 1 and column 14 lines 57-67 and column 15 lines 1-3).

Juitt does not explicitly disclose a centralized infrastructure integrated into said distributed authentication infrastructure. Doshi discloses a centralized infrastructure integrated into said distributed authentication infrastructure (Doshi: see figure 6 and Abstract section). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of a hybrid centralized/distributed of Doshi into the method of Juitt to prevent the scalability and bottleneck problems typically associated with fully centralized approaches (Doshi: column 34 lines 44-46).

6. Regarding claims 2 and 36, Juitt further discloses wherein said plurality of nodes includes a verifying node coupled to a new entity for verifying the identification of said

new entity and enrolling said new entity into the hybrid authentication system (Juitt: column 15 lines 4-17).

7. Regarding claim 3, Juitt further discloses wherein said new entity provides said verifying node with at least one predetermined credential (Juitt: column 9 lines 53-61).

8. Regarding claims 7 and 11, Juitt further discloses wherein said central server is said new entity (Juitt: see figure 1A).

9. Regarding claim 8, Juitt further discloses wherein said distributed authentication infrastructure requires a quorum of said plurality of nodes for enrolling a new entity into the hybrid authentication system (Juitt: column 3 lines 50-61).

10. Regarding claim 12, Juitt further discloses wherein said central server is coupled to a new entity and is utilized for verifying the identification of said new entity and enrolling said new entity into the hybrid authentication system, said central server producing a log for recording a plurality of failed authentications and a plurality of failed enrollments by said plurality of nodes (Juitt: column 3 lines 50-61 and column 12 lines 61-67 and column 13 lines 1-12).

11. Regarding claim 13, Juitt further discloses wherein said central server is coupled to said plurality of nodes for at least one of issuing a global directive thereto and bolstering said plurality of nodes by assisting with at least one of an enrollment task, an authentication task, and a permission granting task (Juitt: column 16 lines 37-57 and column 3 lines 50-61).

12. Regarding claims 14 and 31, Juitt further discloses wherein said global directive includes at least one of a rekey instruction and a critical trust chain path, said rekey

instruction and said critical trust chain path for providing a secured data transfer line (Juitt: see figure 1A item 125 (i.e., authentication server)).

13. Regarding claims 18 and 22, Juitt further discloses wherein said second node is coupled to a trusted third party node from said plurality of nodes, said second node producing an authentication task signed by said first node and sending said authentication task to said trusted third party node, said trusted third party node verifying said identification of said first node (Juitt: see figure 2).

14. Regarding claim 23, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

15. Regarding claim 24, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

16. Regarding claim 29, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

17. Regarding claim 30, Juitt further discloses wherein said central server is coupled to said plurality of nodes for at least one of issuing a global directive thereto and supporting said plurality of nodes by assisting with at least one of an enrollment task, an authentication task, and a permission granting task (Juitt: column 3 lines 50-61 and column 12 lines 61-67 and column 13 lines 1-12).

18. Regarding claim 32, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

19. Regarding claim 33, Juitt further discloses wherein migrating comprises coupling a central server to said plurality of nodes (Juitt: see figure 1A).

20. Regarding claim 34, Juitt further discloses coupling said central server to a verifying node of said plurality of nodes; sending at least one predetermined credential from said central server to said verifying node; enrolling said central server into the hybrid authentication system (Juitt: see Abstract section and column 12 lines 61-67 and column 13 lines 1-12).
21. Regarding claim 38, Juitt further discloses appointing said central server as a proxy for a quorum of said plurality of nodes and for fulfilling an enrollment task; and enrolling said new entity into the hybrid authentication system (Juitt: see Abstract section and column 12 lines 61-67 and column 13 lines 1-12).
22. Claims 4-6, 9-10, 15-17, 19-21, 25-28, 35 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Juitt in view of Doshi, further in view of Benantar (US 2003/0130947) (hereinafter Ben).
23. Regarding claim 4, Juitt in view of Doshi does not explicit disclose wherein said verifying node signs a certificate related to said new entity. Ben discloses wherein said verifying node signs a certificate related to said new entity (Ben: column 1 paragraph [0012]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of the certificate of Ben into the method of Juitt in view of Doshi to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).
24. Regarding claims 5, 17 and 20, Juitt in view of Doshi does not explicit disclose wherein said central server publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has

been revoked. Ben discloses wherein said central server publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked (Ben: paragraphs [0043, 0047 and 0057]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of the certificate revocation list of Ben into the method of Juitt in view of Doshi to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

25. Regarding claims 6, 10, 16 and 21, Juitt in view of Doshi does not explicitly disclose wherein a quorum of said plurality of nodes publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked. Ben discloses wherein a quorum of said plurality of nodes publishes a certificate revocation list, said verifying node examining said certificate revocation list for determining whether said certificate has been revoked (Ben: paragraphs [0043, 0047 and 0057]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of the certificate revocation list of Ben into the method of Juitt in view of Doshi to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

26. Regarding claim 9, Juitt in view of Doshi does not explicitly disclose wherein each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature. Ben discloses wherein

each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature (Ben: paragraphs [0008 and 0037]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of signing a certificate of Ben into the method of Juitt in view of Doshi to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

27. Regarding claims 15 and 19, Juitt in view of Doshi does not explicit disclose wherein said plurality of nodes includes a first node and a second node coupled to said first node, said first node presenting a first certificate to said second node for authenticating said first node. Ben discloses wherein said plurality of nodes includes a first node and a second node coupled to said first node, said first node presenting a first certificate to said second node for authenticating said first node (Ben: paragraphs [0008 and 0045]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of using a certificate of Ben into the method of Juitt in view of Doshi to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

28. Regarding claims 25-27, Juitt in view of Doshi does not explicit disclose wherein said plurality of nodes is a plurality of members including a first member and a second member, said certificate authority issuing a first group certificate to said first member that provides said first member with a first permission level, said certificate authority

issuing a second group certificate to said second member that provides said second member with a second permission level. Ben discloses wherein said plurality of nodes is a plurality of members including a first member and a second member, said certificate authority issuing a first group certificate to said first member that provides said first member with a first permission level, said certificate authority issuing a second group certificate to said second member that provides said second member with a second permission level (Ben: see Abstract section). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of using a certificate of Ben into the method of Juitt in view of Doshi to have a method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

29. Regarding claim 28, Juitt further discloses wherein said first permission level is greater than said second permission level (Juitt: see figure 6).

30. Regarding claims 35 and 37, Juitt in view of Doshi does not explicit disclose coupling said central server to a verifying node of said plurality of nodes; sending a certificate revocation list from said central server to said verifying node; enrolling said central server into the hybrid authentication system. Ben discloses coupling said central server to a verifying node of said plurality of nodes; sending a certificate revocation list from said central server to said verifying node; enrolling said central server into the hybrid authentication system (Ben: see Abstract section and paragraph [0043]). Therefore, it would have been obvious to one ordinary skill in the art to apply the teaching of using a certificate of Ben into the method of Juitt in view of Doshi to have a

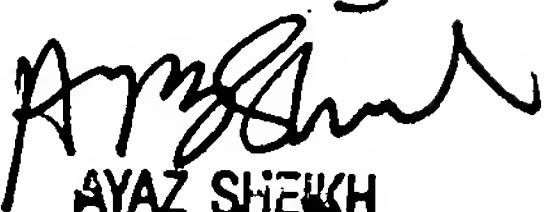
method and system that simplifies the administrative processing associated with the trust paths that are required for valid use of digital certificates (Ben: paragraph [0011]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Trang Doan  
Examiner  
Art Unit 2131

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

T.D.  
03/30/2007